Privacy Impact Assessment

eIDAS-koppelpunt

Auteurs: mr.drs. J.H.J. Terstegge CIPP E/US
dr. J.A.G. Versmissen CIPP/E
mw. T.N. Tran LLB

Datum: 31 juli 2015
Versie: 1.0
Pagina's: 43

Disclaimer

Dit Privacy Impact Assessment (PIA) is uitgevoerd op een moment dat een groot deel van de voor een PIA benodigde informatie nog niet beschikbaar was.
Het gevolg hiervan is dat deze PIA meer het karakter heeft van een *verkennend onderzoek* ten behoeve van verdere beleids- en besluitvorming dan van een volwaardige risicoanalyse op een min of meer voldragen implementatieplan. Dit was ook uitdrukkelijk de bedoeling van de opdrachtgever. De resultaten van deze analyse zullen door de opdrachtgever verwerkt worden in de memorie van toelichting bij het wetsvoorstel Uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten. De Rijksoverheid zal de resultaten van de PIA tevens gebruiken bij het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van het eIDAS-koppelpunt. Daarnaast kan de opdrachtgever de resultaten van de PIA gebruiken om te bevorderen dat de vereiste bestuurlijke, juridische, technische en praktische aanpassingen worden gedaan met als einddoel een goede uitvoering van de eIDAS-verordening.

Privacy Management Partners

Princenhof Park 9
3872 NG Driebergen

Postbus 1200
3970 BE Driebergen

Telefoon: 085 401 3866
E-mail: info@pmpartners.nl
Internet: www.pmpartners.nl

Inhoudsopgave

Begrippenlijst

In dit document verstaan onder:

- eIDAS-koppelpunt: Het koppelpunt als bedoeld in artikel 2(1) van de implementatieverordening (*concept*) inzake het interoperabiliteit raamwerk ter uitvoering van artikel 12(8) van Verordening 910/2014 van het Europese Parlement en van de Raad inzake elektronische identificatie en vertrouwensdiensten voor de elektronische transacties in de interne markt (Uitvoeringsverordening Interoperabiliteit);

- Persoonsgegeven: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub a Wbp);

- Verwerking: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (art. 1 sub b Wbp);

- Verantwoordelijke: De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (art. 1 sub d Wbp);

- Bewerker: Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (art. 1 sub e Wbp);

- Betrokkene: Degene op wie een persoonsgegeven betrekking heeft (art. 1 sub f Wbp);

- Toestemming: Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt (art. 1 sub i Wbp);

- Beveiliging: Passende technische en organisatorische maatregelen om persoonsgegevens – gelet op de risico's die de verwerking, de aard van de te beschermen persoonsgegevens, de stand van de techniek en de kosten van de tenuitvoerlegging – te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (art. 13 lid 1 Wbp).

Hoofdstuk 1 – Inleiding

De op 18 september 2014 in werking getreden EU-verordening 910/2014 elektronische identiteiten en vertrouwensdiensten (hierna: "eIDAS-verordening" of hierna kortweg "de verordening") regelt onder andere de wederzijdse erkenning tussen lidstaten van elektronische identiteiten. De verordening schrijft voor dat vanaf 2018 gebruik van nationale elektronische identiteiten in het buitenland mogelijk wordt, zodat burgers en ondernemers eenvoudiger diensten kunnen afnemen en veilig transacties kunnen verrichten via websites van buitenlandse overheden. Gegevensbescherming is bij de verordening elektronische identiteiten en vertrouwensdiensten een belangrijk aandachtspunt.

Het Ministerie van Economische Zaken (hierna: "EZ") is dossierhouder van de eIDAS-verordening en tevens beleidsverantwoordelijk. Om de verordening in te passen in het Nederlands recht is een implementatiewet vereist. De implementatiewet omvat wijzigingen van een aantal andere wetten; de Telecomwet, de Algemene wet bestuursrecht, het Burgerlijk Wetboek en de Wet bescherming persoonsgegevens.

Gegevensbescherming bij de verordening elektronische identiteiten en vertrouwensdiensten is een belangrijk aandachtspunt. Het wetsvoorstel voor de implementatiewet concentreert op de wijze waarop een buitenlandse burger of bedrijf zich moet identificeren waarbij de minister als verantwoordelijke persoonsgegevens verwerkt.

Het wetsvoorstel is neergelegd in het wetsvoorstel uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten (hierna: "wetsvoorstel"). Voor dit wetsvoorstel is een Privacy Impact Assessment (hierna: "PIA") benodigd op het eIDAS-koppelpunt.

EZ heeft Privacy Management Partners gevraagd een PIA uit te voeren op het eIDAS-koppelpunt dat als gevolg van de verordening in Nederland wordt ingevoerd. Het onderhavige rapport bevat de resultaten daarvan. Deze zullen door EZ verwerkt worden in de memorie van toelichting bij het wetsvoorstel. De Rijksoverheid zal de resultaten van de PIA tevens gebruiken bij het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van het eIDAS-koppelpunt. Daarnaast kan de Rijksoverheid de resultaten van de PIA gebruiken om te bevorderen dat de vereiste bestuurlijke, juridische, technische en praktische aanpassingen worden gedaan met als einddoel een goede uitvoering van de verordening.

Hoofdstuk 2 – Reikwijdte van deze PIA

Om grensoverschrijdend gebruik van elektronische identificatiemiddelen mogelijk te maken, is een technische voorziening nodig die berichten kan versturen over elektronische identiteiten verstrekt in Nederland en berichten kan ontvangen over elektronische identiteiten verstrekt in andere lidstaten (eIDAS-koppelpunt). Deze voorziening stuurt persoonsidentificatie gegevens van burgers en bedrijven uit andere lidstaten naar Nederlandse openbare instanties die deze nodig hebben voor toegangsverlening tot – en indien positief – het verlenen van online dienstverlening aan deze groep. Andersom stuurt de voorziening persoonsidentificatie gegevens van Nederlandse burgers en bedrijven naar openbare instanties in andere lidstaten, waar deze burgers en bedrijven online diensten willen afnemen (indien althans tot melding van een Nederlands stelsel bij de Europese Commissie wordt overgegaan).

Het eIDAS-koppelpunt (ook wel de 'eIDAS-node' genoemd) zal worden aangesloten op het Nederlandse eID-stelsel[1]. Het koppelpunt wisselt persoonsidentificatie gegevens uit met enerzijds de koppelpunten van andere Lidstaten en anderzijds het eID-stelsel.[2]

> NB. De referentie-implementatie van het eIDAS-koppelpunt wordt ontwikkeld door de Europese Commissie, Directoraat-Generaal Informatica (DIGIT).[3] Nederland is voornemens om deze referentie-implementatie over te nemen.

Deze PIA richt zich primair op de verwerkingen zoals die zullen gaan plaatsvinden via het Nederlandse eIDAS-koppelpunt. Het gaat dan zowel om inkomende berichten (dus vanuit het buitenland) als om uitgaande berichten (dus naar het buitenland).

Beperkingen in de reikwijdte van deze PIA

Ketenissues out-of-scope

Het koppelpunt maakt onderdeel uit van een grotere verwerkingsketen, die door Europees recht wordt gereguleerd. De verwerkingen buiten het koppelpunt vallen echter nadrukkelijk buiten de scope van deze PIA. Het gaat in het bijzonder om de volgende aspecten:

- De eIDAS-verordening werkt rechtstreeks in Nederland en is dus van invloed op de verwerkingen die via het eIDAS-koppelpunt plaatsvinden. De verordening zelf en de daaruit voortvloeiende rechten en verplichtingen van de betrokken partijen zijn voor Nederland echter een gegeven. De privacyaspecten van de door de eIDAS-verordening

[1] Dit rapport gebruikt de term eID-stelsel. Inmiddels is het stelsel omgedoopt tot Idensys.

[2] NB. Niet alle Lidstaten zullen een nationaal koppelpunt inrichten. Sommige Lidstaten, zoals Duitsland en Oostenrijk, kiezen er voor om een stukje software bij de koppelpunten van de andere Lidstaten te plaatsen (de zogeheten 'middleware oplossing').

[3] Het eIDAS-stelsel vindt zijn oorsprong in het Europese onderzoekproject STORK (zie www.eid-stork.eu en www.eid-stork2.eu). In het STORK-project staat de oplossing die Nederland zal gaan invoeren bekend als "PEPS" (Pan-Europese proxy server). Een andere variant is de Middleware oplossing, waarbij een stukje software van land A op de server van land B wordt geplaatst. De Artikel 29 Werkgroep heeft met betrekking tot de STORK-oplossing een aantal aanbevelingen gedaan, maar merkt op dat er op het ontwerp geen PIA is uitgevoerd (brief van 15 april 2011, just.c3(2011) 471117). Voor de volledigheid is de brief met de aanbevelingen van de Artikel 29 Werkgroep opgenomen als Bijlage 4.

bestreken materie hebben wij daarom buiten de reikwijdte van deze PIA gehouden.[4]

- Bij de gegevensverwerking via het eIDAS-koppelpunt gaat het, naast het verzenden van Nederlandse identificatiegegevens naar andere Lidstaten, om de aanvaarding van buitenlandse elektronische identiteiten door Nederlandse overheden. De authenticatie zelf vindt echter plaats onder verantwoordelijkheid van de desbetreffende andere Lidstaat, en valt daarmee buiten de reikwijdte van deze PIA. Dat geldt ook voor de juistheid van de uit het buitenland ontvangen en naar het buitenland verzonden gegevens.

- De persoonsgegevens die via het eIDAS-koppelpunt worden doorgegeven, zijn bedoeld om gebruikt te worden door een (overheids)dienstverlener. Het gebruik dat dergelijke (overheids)dienstverleners vervolgens van de gegevens maken, valt uitdrukkelijk buiten de reikwijdte van deze PIA.

- Het eIDAS-koppelpunt zal ook gegevens gaan uitwisselen met Turkije. Op verzoek van opdrachtgever valt dit internationale gegevensverkeer evenwel buiten de reikwijdte van deze PIA.

    - **Opmerking**: Artikelen 76 en 77 Wbp bevatten een regeling voor internationaal gegevensverkeer op grond waarvan doorgifte van persoonsgegevens naar ontvangers buiten de Europese Economische Ruimte (EER) is verboden, tenzij een van de in deze artikelen genoemde uitzonderingen van toepassing is. De meest voor de hand liggende mogelijkheden voor doorgifte van persoonsgegevens vanuit Nederland naar Turkije zijn:

        - Een verdrag tussen de EU en Turkije waarmee de Europese en Turkse stelsels op elkaar worden aangesloten waarin afspraken staan waarmee een passend beschermingsniveau wordt gegarandeerd (art. 76 Wbp), of

        - Toestemming van de betrokkene voor de doorgifte van zijn/haar persoonsgegevens in het specifieke geval (art. 77 lid 1 sub a Wbp).[5]

Toekomstige ontwikkelingen

Een groot aantal zaken waren nog in ontwikkeling op het moment dat de PIA werd uitgevoerd. Derhalve kunnen wij geen of slechts beperkt uitspraken doen over de privacyaspecten van het koppelpunt als het gaat om die toekomstige ontwikkelingen.

- De referentie-implementatie en de software voor het eIDAS-koppelpunt worden ontwikkeld door de Europese Commissie. Deze waren ten tijde van de uitvoering van deze PIA nog niet beschikbaar. Wij kunnen derhalve geen uitspraken doen over de privacy- en securityaspecten van de referentie-implementatie of de software (zie ook

[4] Het uitvoeren van een PIA op het Europese eID-stelsel en de interoperabiliteit is primair de taak van de Europese Commissie en/of het STORK-project.

[5] NB. Anders dan doorgiften naar andere EER-lidstaten, staat artikelen 76 en 77 Wbp de doorgifte naar een land buiten de EER niet toe op basis van een wettelijke verplichting van een niet-EER land of de taak van een bestuursorgaan van een niet-EER land.

Aanbeveling 2 in Hoofdstuk 6).

- Ten tijde van het onderzoek was er nog geen definitieve keuze gemaakt omtrent de vraag of het eIDAS-koppelpunt bij EZ zou worden ondergebracht of dat het zou worden ondergebracht bij een of meerdere deelnemers aan het eID-stelsel ('eID-makelaars'), waarbij in het laatste geval sprake is van hosting bij een private partij. Wij kunnen derhalve slechts beperkt uitspraken doen over de specifieke privacy- en securityaspecten van de uiteindelijke hosting-oplossing (zie Aanbeveling 1 in Hoofdstuk 6);

- De eIDAS-verordening schrijft uitwisseling van een minimale dataset voor. Dit zijn attributen die elke lidstaat na authenticatie moet aanleveren. Daarnaast definieert de verordening optionele attributen die landen *mogen* uitwisselen. Deze attributen kunnen in de toekomst verder worden uitgebreid met andere aanvullende attributen, maar er was op het moment van het onderzoek nog geen zicht op de vraag óf Nederland dergelijke aanvullende attributen zal gaan invoeren en zo ja welke. Derhalve kunnen wij geen uitspraken doen over de privacyaspecten van deze eventuele toekomstige attributen (zie Aanbeveling 10 in Hoofdstuk 6);

- Het eIDAS-koppelpunt in Nederland wordt in eerste instantie alleen opengesteld voor publieke dienstverleners. Het is echter niet uitgesloten dat in de toekomst ook private partijen gebruik kunnen maken van authenticatiediensten via het eIDAS-koppelpunt. Dit toekomstig gebruik valt evenwel buiten de reikwijdte van deze PIA (zie Aanbeveling 6 in Hoofdstuk 6).

Hoofdstuk 3 – Verantwoording

Ter voorbereiding van het onderzoek hebben de onderzoekers zich verdiept in de beschikbare documentatie, waaronder:

- de eIDAS-verordening en daarbij behorende concept-uitvoeringsregelingen;
- het concept van de Wet uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten en de Memorie van Toelichting daarbij;
- Deliverable D2.2 over de juridische aspecten van het STORK 1 project;
- Deliverable 4.2 over de eID datastromen van het STORK 1 project
- Deliverable 3.7 over privacyaspecten van het STORK 2.0 project;
- de brief en het rapport van de Artikel 29 Werkgroep[6] van 15 april 2011 over de STORK-oplossing; en
- de technische en functionele specificaties opgeleverd door het STORK-project.

Vervolgens zijn er gesprekken gevoerd en is er een PIA-workshop gehouden met vertegenwoordigers van het Ministerie van Economische Zaken. Deze PIA is uitgevoerd aan de hand van het Toetsmodel PIA Rijksdienst, een voor de Rijksoverheid verplicht instrument. Het toetsmodel bestaat uit een vragenlijst (deel B) en een verklarend deel (deel A). Er is voor gekozen om de vragenlijst vooraf in te laten vullen door de vertegenwoordigers van EZ en deze vervolgens verder aan te vullen of te verduidelijken tijdens een PIA-workshop onder begeleiding van Privacy Management Partners. De vragenlijst en de bijbehorende antwoorden zijn opgenomen in Bijlage 1.

De resultaten van de vragenlijst zijn verwerkt in een conceptversie van het onderhavige rapport. Dit concept was onderwerp van een validatieworkshop met vertegenwoordigers van EZ. Op basis van de feedback uit deze tweede workshop is van het rapport een nieuwe conceptversie opgesteld. Ten slotte heeft nog een mondeling overleg plaatsgevonden met de opdrachtgever in aanwezigheid een medewerker van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Op basis van deze feedback is het rapport vervolgens gefinaliseerd.

Vanuit EZ waren betrokken:

- drs. F.J.M. van Krevel
- drs. J.W. van der Burght
- drs. I. Vennekens

Vanuit BZK was betrokken:

- ir. J. Stienen

[6] De Artikel 29 Werkgroep is een in de Europese privacyrichtlijn 95/46 ingestelde werkgroep waarin de nationale privacytoezichthouders van de lidstaten en de European Data Protection Supervisor deelnemen.

Hoofdstuk 4 – Beschrijving van het eIDAS-koppelpunt

Dit hoofdstuk beschrijft het eIDAS-koppelpunt en de bijbehorende verwerkingen in termen van de Wbp (zie voor een beknopt overzicht . Deze beschrijving is gebaseerd op de antwoorden op de vragenlijst van het Toetsmodel PIA Rijksdienst en aanvullende mondelinge mededelingen vanuit EZ.

1. Actoren, rollen en gegevensverwerkingen

De volgens actoren zijn betrokken in de onderstaande rollen:[7]

- Nederlands eIDAS-koppelpunt[8]
  - Doorsturen van identiteitsgegevens ter verschaffing van toegang tot elektronische buitenlandse overheidsdiensten door koppeling aan het eID stelsel;
  - Via het eID stelsel doorsturen van identiteitsgegevens van buitenlandse personen naar Nederlandse (overheids)dienstverleners;
  - Koppelen van buitenlandse (EU/EER) eIDAS-nodes (via het Nederlandse eIDAS-koppelpunt zelf) aan het Nederlandse e-ID stelsel;
  - Heeft een audit/monitoring functie om het eIDAS-koppelpunt technisch fit te houden;
  - (Indien nodig) vragen om toestemming voor de verwerking van persoonsgegevens (eIDAS-node/overheidsdienstverlener).

  Rol onder de Wbp: Het is momenteel nog onduidelijk wie voor het koppelpunt als verantwoordelijke in de zin van de Wbp dient te worden aangemerkt. Zie onze opmerkingen en voorstellen daarvoor in Hoofdstuk 5 en 6.

- Burgers/Ondernemers in EU/EER lidstaten
  - *Burgers met Nederlandse identiteit:* Het via de Nederlandse eIDAS-node doen van elektronische verzoeken voor toegang tot buitenlandse overheidsdiensten;
  - *Burgers met overige EU/EER identiteit:* Het – via een buitenlandse eIDAS-node – doen van elektronische verzoeken voor toegang tot Nederlandse overheidsdiensten;
  - (Indien nodig) toestemming geven tot elektronische verzending en verwerking van (ingevoerde) persoonsgegevens.

  Rol onder de Wbp: De burgers c.q. ondernemers (voor zover de laatsten geen rechtspersoon zijn) zijn betrokkenen in de zin van de Wbp.

---

[7] De laatste taak in de genoemde rollen heeft telkens te maken met het verlenen van toestemming door de betrokken burger. Die taak is overgenomen uit het Stork-project. Het is echter zeer de vraag of het vragen van toestemming wel noodzakelijk is. Zie hiervoor de toelichting bij punt 3 in de paragraaf "Compliance" in hoofdstuk 5.

[8] Er moet rekening gehouden worden met de mogelijkheid dat de versleutelde data via de browser doorgeleid worden van de identiteitsdienstverlener naar de e-overheidsdienstverlener zonder dat de eIDAS node 'fysiek' de data door hoeft te sturen. De transmissie wordt wel geregistreerd (logging) door de eIDAS node. Technisch gezien is de node dan geen doorgeefluik, maar een soort 'identiteitsregisseur'. De node verzorgt dan het versturen van de identificaties naar de browser, zodra hij hoort naar welke dienstverlener het verzoek moet. Het is vooralsnog onduidelijk of de data ook 'fysiek' langs de eIDAS node zal gaan (waarschijnlijk niet, maar zolang de Europese software niet klaar is, kan dat niet worden vastgesteld).

- (Buitenlandse) Overheidsdienstverleners
    - o Verstrekken toegang tot hun diensten aan (buitenlandse) burgers/bedrijven;
    - o Verwerking (waaronder pseudonimisering/versleuteling) van persoonsgegevens;
    - o (Indien nodig) vragen om user consent ter verwerking van persoonsgegevens.

  Rol onder de Wbp: De overheidsdienstverleners zijn verantwoordelijke voor de persoonsgegevens gegevens die zij in het kader van hun taken/diensten verwerken. Voor zover het overheidsdienstverleners betreft in andere Lidstaten, zijn zij verantwoordelijke onder hun eigen dataprotectierecht. Zie voor de vraag of zij ook verantwoordelijke zijn voor de verwerkingen via het eIDAS-koppelpunt onze opmerkingen in Hoofdstuk 5.

2. Persoonsgegevens

2a. Gewone persoonsgegevens
Voor de identificatie van burgers (natuurlijke personen) geldt het volgende.

Het eIDAS-koppelpunt routeert berichten die afkomstig zijn van onder de eIDAS-verordening erkende stelsels voor elektronische identificatie. De Uitvoeringsverordening Interoperabiliteit bepaalt dat deze berichten met het oog op het uniek aanduiden van de burger die een dienst wil afnemen bepaalde gegevens *moet* bevatten, en daarnaast enkele aanvullende gegevens *mag* bevatten.[9] In het STORK-project is het mogelijk om nog meer gegevens te routeren (bijvoorbeeld “student”), maar deze vallen buiten beschouwing van dit hoofdstuk (zie ook de opmerkingen onder het volgende punt, “bijzondere gegevens”).

De berichten *moeten* de volgende gegevens bevatten ter unieke aanduiding van de betreffende burger:

- Achternaam
- voornaam/-namen
- geboortedatum
- unieke identifier[10]

De gegevens die berichten in aanvulling daarop *mogen* bevatten ter unieke aanduiding van de betreffende burger zijn:

- voor- en achternamen bij geboorte
- geboorteplaats
- huidig (woon)adres

---

[9] Aan het betreffende stelsel is de keuze of het gegevens uit de lijst van optionele identificerende gegevens in zijn berichten opneemt, en zo ja, welke.

[10] Verplicht onderdeel van de hierboven beschreven minimale gegevensset ter aanduiding van een natuurlijke persoon is “a unique identifier constructed by the sending Member State [...] which is as persistent as possible in time.” Een in de tijd zo onveranderlijk mogelijk unieke identifier brengt privacyrisico’s met zich mee, aangezien deze het koppelen van persoonsgegevens vergemakkelijkt (Article 1 of the draft Annex to the Commission Implementing Regulation on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 9190/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market).

- geslacht

NB. Er is ook een minimum dataset voorgeschreven voor 'rechtspersonen'. Deze dataset bevat naast de naam en adres van het bedrijf ook het BTW-nummer en andere belastingidentificatienummers. Wij wijzen er op dat ook gegevens met betrekking tot bedrijven die niet in de vorm van een rechtspersoon worden gedreven, kwalificeren als persoonsgegevens. Hoewel de eIDAS-regelgeving zich alleen lijkt te beperken tot 'natuurlijke' personen en 'rechtspersonen', kan het in de praktijk zo zijn dat ondernemers die geen rechtspersoon vertegenwoordigen toch de categorie 'rechtspersonen' kiezen om zich als bedrijf te identificeren. In dat geval worden dus ook persoonsgegevens verwerkt.

Al deze gegevens kwalificeren als persoonsgegevens in de zin van de Wbp. Met de mogelijke uitzondering van de unieke identifier (zie punt 2c hieronder) kwalificeren al deze gegevens als 'gewone persoonsgegevens', d.w.z. persoonsgegevens waar geen bijzondere privacygevoeligheid aan kleeft. Bovendien is het zo dat deze gegevens het koppelpunt slechts in versleutelde vorm passeren (zie ook paragraaf 9 *Beveiliging* hieronder).

2b. Bijzondere gegevens

Er zullen door het eIDAS-koppelpunt vooralsnog geen bijzondere gegevens worden verwerkt.

NB. Het kan – afhankelijk van de dienst met het oog waarop authenticatie plaatsvindt – nuttig zijn dat andere gegevens over de burger vanuit het stelsel voor identificatie via een bericht geleverd worden. De eIDAS-verordening bevat daarvoor geen regeling[11], maar sluit deze mogelijkheid ook niet uit. Integendeel, artikel 8 van de Uitvoeringshandeling Interoperabiliteit bepaalt dat de door de koppelpunten te gebruiken gemeenschappelijke berichtopbouw *"[allows] the flexibility to meet the needs of additional attributes relating to identification"*.

Er dient daardoor vanuit te worden gegaan dat ook berichten met dergelijke 'additionele attributen' het koppelpunt zullen passeren. Het koppelpunt heeft hierover namelijk geen controle, aangezien het al dan niet gebruiken van deze attributen een aangelegenheid is tussen de dienstverlener, de identificatiedienstverlener en de burger in kwestie. Deze attributen zullen vrijwel zonder uitzondering kwalificeren als persoonsgegevens, aangezien zij juist tot doel hebben om additionele informatie over de burger in kwestie te verschaffen. Het is niet uit te sluiten, en voor bepaalde toepassingen zelfs heel waarschijnlijk, dat het daarbij ook gaat om bijzondere persoonsgegevens als bedoeld in artikel 16 Wbp.

2c. BSN/voorgeschreven identiteitsnummers

Richtlijn 95/46/EG bepaalt dat de lidstaten "de voorwaarden vast[stellen] waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt". Dit is in Nederland neergelegd in artikel 24 Wbp en onder meer nader uitgewerkt in een aantal wetten omtrent het gebruik van het Burger Service Nummer (BSN). In beginsel is het mogelijk dat ook andere lidstaten het gebruik van zulke persoonsnummers toestaan. Volgens de eIDAS-specificaties kunnen zulke nummers gepseudonimiseerd worden alvorens via de eIDAS-node te worden verwerkt. Nederland heeft er voor gekozen om bij elektronische identificatie van burgers binnen eIDAS-verband niet het BSN als zodanig te gebruiken, maar een daarvan afgeleid pseudoniem.

NB. Wij wijzen er hier op dat het gebruik van pseudoniemen niet betekent dat de Wbp niet meer van toepassing is. Als aan de hand van een pseudoniem een persoon uniek kan worden aangewezen in de

[11] Wel als het gaat om certificaten, maar alleen voor certificaten verbonden aan vertrouwensdiensten, en daar valt elektronische identificatie niet onder.

groep, is ook het pseudoniem een persoonsgegeven.[12] Dat zal in de context van een eIDAS zeker het geval zijn.

NB2. Daarnaast speelt de vraag of het BSN gebruikt mag worden om een andere unieke identifier te creëren.[13] Het verbod van artikel 24 Wbp op gebruik van het BSN voor andere doeleinden dan die in de wet genoemd zijn, staat daar immers in beginsel aan in de weg. Dit probleem zou echter niet spelen als de omzetting van het BSN voor eIDAS-doeleinden in een wettelijk kader wordt gegoten.

2d. Persoonsgegevens m.b.t. gedrag, aanwezigheid of prestaties

Er worden door het eIDAS-koppelpunt alleen loggegevens over gebruikers opgeslagen. Dergelijke gegevens kwalificeren als persoonsgegevens met betrekking tot het gedrag of aanwezigheid van gebruikers. De Wbp stelt geen specifieke eisen aan de verwerking van dit soort gegevens, maar naar hun aard hebben dergelijke gegevens een hogere gevoeligheid en de beveiligingsmaatregelen dienen derhalve van een bij de gevoeligheid passend niveau te zijn (art. 13 Wbp).

3. Doeleinden van de verwerking

Het inrichten van een eIDAS-koppelpunt is een expliciete verplichting uit de eIDAS-verordening en de daarmee samenhangende uitvoeringsverordeningen en daarmee is het doel van het koppelpunt legitiem en welbepaald (art. 7 Wbp).

Het doel van de verwerking door het eIDAS-koppelpunt kan als volgt worden omschreven:

> *Het faciliteren van grensoverschrijdende dienstverlening binnen de EU/EER door het routeren van het daarvoor benodigde gegevensverkeer over authenticatie (authenticatiedienst) van burgers en bedrijven richting overheidsdienstverleners, en in de toekomst mogelijk ook naar private partijen, opdat deze burgers en bedrijven zich kunnen authentiseren met hun nationale identificatiemiddel.*[14]

---

[12] Zie ook pagina 14 van het Advies van 20 juni 2007 van de Artikel 29 Werkgroep inzake het begrip persoonsgegeven (WP136). In haar advies inzake anonimiseringstechnieken van 10 april 2014 (WP216) in de Artikel 29 Werkgroep uitgebreid ingegaan op pseudoniemen: *"Pseudonymisation consists of replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymisation when used alone will not result in an anonymous dataset. Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation.. [….] Pseudonymised data cannot be equated to anonymised information as they continue to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection. This is especially relevant in the context of scientific, statistical or historical research. [….] Extra steps should be taken in order to consider the dataset as anonymised, including removing and generalising attributes or deleting the original data or at least bringing them to a highly aggregated level. [….] In this regard it is necessary to warn on the use of pseudonyms as a way to afford adequate protection to data subjects against identity or attribute leaks. If pseudonymisation is based on the substitution of an identity by another unique code, the presumption that this constitutes a robust de-identification is naïf and does not take into account the complexity of identification methodologies and the multifarious contexts where they might be applied."* De Artikel 29 Werkgroep ziet pseudonimisering niettemin als een belangrijke beveiligingsmaatregel.

[13] Dit is bijvoorbeeld het geval bij het persoonsgebonden onderwijsnummer en het BTW-nummer van ZZP-ers.

[14] Deze doelomschrijving kan worden gebruikt bij de melding ex artikel 27 Wbp.

4. Grondslag van de verwerking

In het STORK-ontwerp was voorzien in het vragen van toestemming van de burger voor het verwerken van zijn persoonsgegevens via het koppelpunt. Naar ons oordeel is dat niet nodig voor de verwerkingen via het eIDAS-koppelpunt.

Bij (het faciliteren van) publieke onlinediensten zal de grondslag voor de gegevensverwerking door het eIDAS-koppelpunt in beginsel dezelfde zijn als de grondslag die door de overheidsinstantie wordt gebruikt om de gegevensverwerking te rechtvaardigen. Overheidsinstanties verwerken persoonsgegevens van burgers primair op grond van een wettelijke plicht (art. 8 sub c Wbp) of de noodzaak voor de goede vervulling van hun publieke taak (art. 8 sub e Wbp). In het laatste geval is het uitgangspunt dat de gegevens worden verwerkt, tenzij de burger bezwaar maakt (art. 8 sub e Wbp juncto art. 40 lid 1 Wbp). Het is niet alleen ongebruikelijk dat de overheid om toestemming vraagt om de gegevens van burgers te verwerken, in gevallen waar de burger feitelijk geen reële mogelijkheid heeft om 'nee' te zeggen tegen de overheid is de toestemming zelfs ongeldig (art. 1 sub i Wbp).

5. Dataminimalisatie

Het principe van dataminimalisatie is stevig verankerd in de eIDAS-verordening. Zoals onder paragraaf 2a van dit hoofdstuk is aangegeven, is een beperkte set gegevens vastgesteld die nodig zijn met het oog op het uniek aanduiden van burgers. Voorts bepaalt artikel 6 lid 2 van de Uitvoeringshandeling Interoperabiliteit dat het koppelpunt geen gegevens mag opslaan, met uitzondering van loggegevens met het oog op het reconstrueren van transacties in het geval van incidenten.

6. Datakwaliteit

De eIDAS-verordening bepaalt dat als een Lidstaat tot melding van zijn stelsel bij de Europese Commissie overgaat, die Lidstaat de juistheid van de persoonsidentificatiegegevens waarborgt (artikel 7d, van de verordening) en de partij die het elektronische identificatiemiddel uitgeeft, verantwoordelijk is voor de koppeling tussen het middel en de identificatiegegevens van een persoon (artikel 7e, van de verordening).

Het verifiëren van de juistheid van de gegevens is echter geen taak van het eIDAS-koppelpunt. Het geeft de gegevens slechts door. Het adequaat beveiligen van de gegevens, waaronder het garanderen van de integriteit van de verwerkte gegevens, is echter wél een taak van het koppelpunt.[15] Omdat het definitieve koppelpunt nog moet worden gebouwd, kunnen er nu geen uitspraken gedaan worden over de wijze waarop en mate waarin het koppelpunt voldoet aan de Europese en/of Nederlandse normen die relevant zijn voor privacy en informatiebeveiliging.

7. Datagebruik

Het eIDAS-koppelpunt gebruikt zelf geen identiteitsdata; het stuurt ze alleen door.

[15] Daarvoor maakt het niet uit of het koppelpunt verantwoordelijke is of bewerker (zie art. 13 resp. art. 14 lid 1 Wbp).

Wel is het de bedoeling dat de eIDAS-node loggegevens vastlegt om incidenten te kunnen reconstrueren). Ook op deze loggegevens is de Wbp van toepassing. Dat betekent dat de loggegevens alleen voor met de beveiliging verenigbare doeleinden mogen worden gebruikt (art. 9 lid 1 Wbp).

8. Verstrekkingen aan internen/externen

Afhankelijk van hoe lang de encryptieketen is, zal niemand de (versleutelde) persoonsgegevens kunnen inzien, behalve mogelijk alleen de technisch beheerder van het eIDAS-koppelpunt.[16] Deze zal de versleutelde gegevens echter niet kunnen ontsleutelen. Wel heeft de technisch beheerder een monitoring rol en zal deze een audit trail uit moeten kunnen voeren om het koppelpunt technisch fit te houden en incidenten te kunnen managen.

Bijzonder aandachtspunt verdient de situatie waarin het koppelpunt wordt ondergebracht bij een of meerdere eID-makelaars: in hoeverre mogen zulke partijen eisen stellen (en welke dan) aan andere betrokken partijen in de keten?

9. Beveiliging

Uitvoeringshandeling Interoperabiliteit van de Europese Commissie zet de kaders voor de beveiliging van de eIDAS-node. Deze voorschriften zijn echter niet heel erg gedetailleerd en behoeven derhalve nadere invulling in de Nederlandse implementatie.

Indien de eIDAS-node binnen de Rijksoverheid wordt ondergebracht, is de Baseline Informatiebeveiliging Rijksdienst (BIR) relevant. Dat is ook het geval als de eIDAS-node wordt uitbesteed aan een bewerker, waarbij de Minister van EZ verantwoordelijke blijft. De BIR is echter niet van toepassing als de eIDAS-node wordt ondergebracht bij een of meer eID-makelaars die zelf verantwoordelijke zijn. Deze zullen echter ten minste aan de (vage) Europese eisen moeten voldoen. De Minister kan overwegen om zelf aanvullende eisen op het gebied van informatiebeveiliging te stellen aan die makelaar(s), bijvoorbeeld op basis van ISO 27001.[17] Het opleggen van beveiligingseisen is in ieder geval niet ongebruikelijk bij inkoop van diensten waarbij persoonsgegevens betrokken zijn, zelfs als de dienstverlener een verantwoordelijke is.

> NB. De identiteitsgegevens komen via het eIDAS-koppelpunt terecht bij buitenlandse overheidsinstellingen, maar het is onduidelijk hoe sterk of zwak hun informatiebeveiligingsstandaarden/-systemen zijn. De Verordening heeft daarvoor een minimum betrouwbaarheidsniveau vastgesteld. Omdat echter sprake is van een keten, is de keten van beveiliging zo sterk als zijn zwakste schakel. Het eenzijdig nemen van aanvullende beveiligingsmaatregelen heeft dus weinig zin als andere landen niet hetzelfde doen. Echter, omdat de beveiligingseisen uit de gegevensbeschermingswetgeving van de Lidstaten sowieso

[16] Encryptie is mogelijk end-to-end, maar dat kan ook per schakel. In dat laatste geval zal er op het koppelpunt sprake zijn van niet-versleutelde gegevens, waardoor de technisch beheerder deze dus potentieel kan inzien. Overigens is het zo dat de gebruikte encryptie-techniek periodiek geëvalueerd moet worden om te zorgen dat de encryptie passend is en blijft in het licht van de ontwikkeling van de techniek en de daarmee samenhangende risico's van het kraken van de versleuteling.

[17] De project start architectuur van DICTU zou hiervoor mogelijk als basis kunnen dienen.

sterk van elkaar verschillen, dreigt zelfs zonder specifieke eisen in Europa een lappendeken van beveiligingsniveaus te ontstaan (zie Aanbeveling 4 in Hoofdstuk 6).

Het is nog niet bekend of het koppelpunt bij een bewerker zal worden gehost. Indien dit wel het geval is, zal het pakket van beveiligingsmaatregelen een punt van aandacht moeten zijn in de aanbesteding (bij voorkeur een 'knock out'-criterium). De door de bewerker te implementeren beveiligingsmaatregelen zullen voorts moeten worden vastgelegd in een bewerkersovereenkomst (art. 14 lid 5 Wbp) (zie Aanbeveling 5 in Hoofdstuk 6).

10. Bewerker

Het is momenteel nog niet bekend of het koppelpunt bij een bewerker zal worden gehost. Derhalve kunnen op dit punt door ons verder geen uitspraken worden gedaan.

> NB. Het Nederlandse eIDAS-koppelpunt zal wel zelf gaan fungeren als bewerker voor de landen die niet hebben gekozen voor de node-oplossing, maar voor de middleware oplossing (Duitsland en Oostenrijk). In dat geval wordt een stukje Duitse en Oostenrijkse software op de Nederlandse eIDAS-node geplaatst die de aanvragen vanuit/naar Duitsland en Oostenrijk afhandelt. De Nederlandse beheerder van de node fungeert in dat geval als bewerker voor de Duitse c.q. Oostenrijkse overheid. Behalve dat artikel 17 lid 3 van Richtlijn 95/46/EG in zo'n geval voorschrijft dat de Nederlandse beveiligingseisen moeten worden gehanteerd (voor zover relevant in het licht van de Europese beveiligingseisen), valt dit verder buiten de werkingssfeer van de Wbp (want onder het recht van de desbetreffende Lidstaten, art. 4 lid 1 sub a Richtlijn 95/46/EG).

11. Transparantie

De Artikel 29 Werkgroep gaf in haar commentaar op het STORK-project reeds aan dat het van belang was dat de privacyverklaringen die aan de betrokkenen ter beschikking worden gesteld rekening houden met de complexe infrastructuur. Deze privacyverklaringen moeten duidelijk en nauwkeurig beschrijven wat er met de gegevens gebeurt ongeacht het type oplossing dat wordt geboden.

> NB. Omdat het eIDAS-koppelpunt 'onder water' zijn werk doet, ligt het voor de hand dat de door de Artikel 29 Werkgroep bedoelde verklaringen zijn opgenomen in de privacyverklaring van de overheidsdienstverlener die is aangesloten op de eIDAS-infrastructuur (zie Aanbeveling 3 in Hoofdstuk 6).

12. Internationaal gegevensverkeer

In het kader van het eIDAS-koppelpunt vindt geen gegevensverkeer met landen buiten de EU/EER plaats.[18]

---

[18] Behalve mogelijk met Turkije. Op verzoek van de opdrachtgever is Turkije voor deze PIA uitdrukkelijk out-of-scope geplaatst.

Hoofdstuk 5 – Conclusies

I. Samenvatting risico's voor rechten en vrijheden van de betrokkene

In onderstaande tabel treft u een overzicht aan van de mate van de risico's voor fundamentele rechten en vrijheden van de betrokkene bij de verwerking van zijn/haar persoonsgegevens via het eIDAS-koppelpunt.

Leeswijzer: *De eerste kolom betreft de risico's zoals wij deze op dit moment kunnen vaststellen. De tweede kolom betreft de verwachting als de beheerder van het eIDAS-knooppunt geen of onvoldoende maatregelen neemt om de risico's af te dekken of als deze maatregelen falen. De gebruikte kwalificaties zijn:*

- *Hoog (rood):* *De verwerking brengt (zeer) ernstige risico's mee voor het betreffende belang van de betrokkene; de gevolgen zijn ingrijpend en het is onwaarschijnlijk dat ze door menselijk ingrijpen alsnog kunnen worden opgelost;*
- *Substantieel (geel):* *De verwerking brengt een zekere mate van risico's mee voor het betreffende belang van de betrokkene; het is waarschijnlijk dat de gevolgen door menselijk ingrijpen alsnog worden opgelost;*
- *Verwaarloosbaar: (groen)* *De risico's voor het betreffende belang van de betrokkene zijn verwaarloosbaar of afwezig.*

	Risico's voor de betrokkene	Daadwerkelijk niveau van de risico's [19]	Verwacht niveau indien, niet het risico niet wordt gemanaged
1.	Veiligheidsrisico's (persoon/familie)	*Onbekend*	Verwaarloosbaar
2.	Risico op inbreuk op de bescherming van de persoonlijke levenssfeer en familieleven	*Onbekend*	Verwaarloosbaar
3.	Risico op inbreuk op de bescherming van de lichamelijke integriteit	*Onbekend*	Verwaarloosbaar
4.	Risico op aantasting van de geestelijke integriteit	*Onbekend*	Verwaarloosbaar
5.	Risico op onrechtvaardige behandeling	*Onbekend*	**Substantieel**
6.	Risico op ongelijke behandeling/discriminatie	*Onbekend*	Verwaarloosbaar
7.	Risico op beschadiging van reputatie	*Onbekend*	Verwaarloosbaar
8.	Risico voor de autonomie	*Onbekend*	Verwaarloosbaar
9.	Risico op onmenselijke behandeling	*Onbekend*	Verwaarloosbaar
10.	Risico's voor bescherming overige (grond)rechten	*Onbekend*	Verwaarloosbaar
11.	Risico op materiële schade of nadeel	*Onbekend*	**Hoog**

Toelichting

Gebruikers kunnen ernstige schade kunnen ondervinden als er iets mis is met de

[19] Omdat het eIDAS-koppelpunt nog niet operationeel is en omdat er op de Europese referentie-implementatie (voor zover wij weten) geen privacy impact assessment is gedaan, kunnen wij op dit moment geen uitspraken doen over de mate van daadwerkelijke risico's van de implementatie van het eIDAS-knooppunt in Nederland.

vertrouwelijkheid, integriteit of beschikbaarheid van hun online identiteit. Het gaat dan met name om ongerechtvaardigde behandeling en materiële schade.

De volgende scenario's zouden de genoemde gevolgen kunnen hebben:

- *Het eIDAS-koppelpunt geeft de gegevens op onjuiste wijze door.*
  Als de juistheid van de identiteitsgegevens in het geding is als gevolg van integriteitsproblemen bij de doorgifte ervan door het eIDAS-koppelpunt, kan de burger of ondernemer mogelijk terechtkomen in een soort *Kafka*-achtige situatie, waarin een overheidsinstantie in het ene land een onjuiste (vaak negatieve) beslissing neemt ten aanzien van die burger of ondernemer omdat het de gegevens die het van het Nederlandse eIDAS-koppelpunt heeft gekregen vertrouwt. Dit probleem is voor de burger c.q. ondernemer waarschijnlijk onzichtbaar (maar met moeite waarschijnlijk wel oplosbaar).

- *Het eIDAS-koppelpunt is niet beschikbaar*
  Het niet beschikbaar zijn van het koppelpunt door bijvoorbeeld een storing, kan grote gevolgen hebben voor de burger of ondernemer. Denk bijvoorbeeld aan het vanwege de storing niet kunnen halen van een deadline voor een aanvraag voor subsidie of de inschrijving voor een studie.

- *Identiteitsdiefstal als gevolg van het bekend worden van de gegevensset via het eIDAS-koppelpunt*
  Identiteitsdiefstal is een groot probleem, ook op internet. Het feit dat de elektronische identiteitsgegevens via een centrale infrastructuur lopen, maakt het eIDAS-koppelpunt tot een aantrekkelijk doelwit voor cybercriminelen. Ook dit kan leiden tot *Kafka*-achtige situaties voor de burger of ondernemer.[20]

Deze risico's moeten dan ook actief gemanaged worden door de beheerder van het koppelpunt, met name door middel van een passend informatiebeveiligingsbeleid[21] rondom het eIDAS-koppelpunt, waardoor de vertrouwelijkheid, integriteit en de beschikbaarheid van de gegevens wordt gegarandeerd. Indien deze risico's niet gemanaged worden, kunnen de gevolgen naar ons oordeel variëren van **Substantieel** tot **Hoog**.

---

[20] Een goed voorbeeld van zo'n situatie is de casus van een man die onterecht als drugcrimineel te boek stond bij de politie, waardoor andere (overheids)instanties de man systematisch als zodanig behandelden (rapport 2009/199, https://www.nationaleombudsman.nl/rapporten/2009/199#samenvatting).

[21] Zie artikel 13 Wbp en de Richtsnoeren Beveiliging van Persoonsgegevens van het CBP voor de vraag wanneer sprake is van een 'passende beveiliging'. Als het koppelpunt onder de verantwoordelijkheid van de Rijksoverheid wordt geplaatst, zijn ook het Veiligheidsvoorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijksdienst (BIR) van toepassing.

II. Samenvatting compliance met de Wet bescherming persoonsgegevens

Het koppelpunt verwerkt twee typen persoonsgegevens:

- Identiteitsgegevens (doorgifte), en
- Loggegevens (opslag)

Voor beide typen persoonsgegevens hebben we de volgende aandachtspunten op het gebied van compliance met de Nederlandse privacywet- en regelgeving aangetroffen:

Aandachtspunten Wbp	Identiteits-gegevens	Log-gegevens [22]
1. Het is duidelijk wie de verantwoordelijke is voor de verwerkingen van persoonsgegevens via het eIDAS-koppelpunt	**Nee,** dit moet nader worden geregeld	Ja
2. De persoonsgegevens worden verwerkt voor een legitiem doel	Ja	Ja
3. De persoonsgegevens worden op een juiste grondslag verwerkt	Hierover moet een besluit worden genomen dat ook invloed heeft op de technische specificaties	Ja, wettelijk voorschrift, art. 9 lid 3 Uitvoerings-verordening Interopera-biliteit
4. De persoonsgegevens worden niet verwerkt voor onverenigbare doeleinden (tenzij met passende waarborgen)	n.v.t.	n.v.t.
5. De persoonsgegevens zijn toereikend, ter zake dienend en niet bovenmatig	Ja	*Onbekend*
6. De persoonsgegevens worden niet langer bewaard dan nodig	n.v.t.	*Onbekend*
7. De persoonsgegevens zijn juist en nauwkeurig	n.v.t.	*Onbekend*
8. De persoonsgegevens worden door de medewerkers van het eIDAS-koppelpunt op vertrouwelijke wijze verwerkt	*Onbekend*	*Onbekend*
9. De persoonsgegevens worden op een passende organisatorische en technische wijze beveiligd	*Onbekend*	*Onbekend*
10. Er is een risico op datalekken	*Onbekend*	*Onbekend*
11. Er zijn voldoende schriftelijke afspraken met de bewerker	*Onbekend*	*Onbekend*
12. Bijzondere gegevens worden verwerkt in overeenstemming met de wet	n.v.t	n.v.t.
13. Het BSN wordt verwerkt in overeenstemming met de wet	n.v.t.[23]	n.v.t.
14. De verwerking is gemeld bij het CBP of een FG	*Onbekend*	*Onbekend*
15. De betrokkene wordt adequaat geïnformeerd over de verwerking van zijn/haar persoonsgegevens	*Onbekend*	*Onbekend*
16. De betrokkene kan adequaat zijn rechten uitoefenen	Onbekend	*Onbekend*
17. Persoonsgegevens worden verwerkt conform de regels voor internationaal gegevensverkeer	n.v.t.	n.v.t.

[22] Omdat er nog geen concreet voorstel ligt voor de logging, zijn de meeste punten nog onbekend. Voor wat betreft punt nr.1 staat vast dat de verantwoordelijke voor het koppelpunt ook de verantwoordelijke is voor de verwerking van de loggegevens. De grondslag daarvoor is de verplichting ex artikel 9 lid 3 om logging in te zetten in het kader van de beveiliging (art. 8 sub c Wbp). De loggegevens worden in dit rapport verder grotendeels buiten beschouwing gelaten.

[23] Maar zie de opmerkingen hierover in de toelichting onder de tabel.

Toelichting

- *Ad 1: Rol eIDAS-koppelpunt*
  De Wbp maakt bij de verwerking van persoonsgegevens onderscheid tussen de rollen "verantwoordelijke" en "bewerker". De verantwoordelijke is degene die doel en middelen van de verwerking vaststelt, en daarmee feitelijk of juridisch de zeggenschap heeft over de verwerking (regie). Een verwerking kan meerdere verantwoordelijken hebben; ieder voor zijn eigen deel of samen voor het geheel. De bewerker verwerkt persoonsgegevens uitsluitend in opdracht van de verantwoordelijke(n) en onder dienst toezicht en instructies.[24]

  Het is thans onduidelijk wie verantwoordelijke is in de zin van de Wbp voor de verwerking via het eIDAS-koppelpunt. Noch de eIDAS-verordening noch het wetsvoorstel geeft hierop een duidelijk antwoord.[25] (Zie hierover Aanbeveling 1 in Hoofdstuk 6).

- *Ad 2: Legitiem doel*
  Omdat het koppelpunt verplicht is uit hoofde van de eIDAS-verordening, is er een legitiem doel om de identiteitsgegevens via het koppelpunt te verwerken. Dit geldt ook voor de loggegevens.

- *Ad 3: Grondslag*
  In het Stork-project is geconcludeerd dat toestemming door de burger de enig mogelijke grondslag was voor het grensoverschrijdende berichtenverkeer.[26] Dat had

---

[24] De verantwoordelijke is ook aansprakelijk voor schade of nadeel die is ontstaan als bij de doorgifte via het eIDAS-koppelpunt wordt gehandeld in strijd met de voorschriften van de Wbp (art. 49 lid 1 juncto lid 3 Wbp), zoals het onvoldoende nemen van beveiligingsmaatregelen zodat een datalek ontstaat. Dit omvat ook de schade of het nadeel dat veroorzaakt wordt door het handelen c.q. nalaten van een bewerker. Een bewerker is slechts aansprakelijk voor schade ontstaan door zijn eigen werkzaamheid (art. 49 lid 3 Wbp).

[25] Ook het rapport van de Artikel 29 Werkgroep inzake het STORK-project laat in het midden of de beheerder van het eIDAS-koppelpunt ('PEPS' in termen van het STORK-project) een verantwoordelijke is of een bewerker voor de partijen aan wie de gegevens worden doorgegeven. Volgens de Artikel 29 Werkgroep is voor beide rollen iets te zeggen. *"In the PEPS model it can be argued that the PEPS is a data controller as far as the electronic identity management is concerned. He processes personal data, transfers them to another PEPS and also handles the replies (signed IDs or rejection). Although the PEPS is a service provided to different institutions (service providers), these are not in control or what happens in de PEPS. The only thing [they are] in control of is to either accept or refuse the offer of a PEPS provider. It can also be argued that the service provider as a controller of the service provided to the citizen chooses to use the services of a PEPS and therefore the PEPS is only a processor acting on behalf of the service provider. This interpretation has one practical disadvantage from the point of view of the aim of reducing administrative burdens. If a PEPS is considered as processor this creates a significant number of controllers of this PEPS (all that use this PEPS). This is a typical dilemma that comes with the phenomena of "electronic portals". The [Article 29 Working Party] did not come to a conclusion in WP 169... In line with WP 169 the subgroup wasn't able to come to a concordant conclusion.... Therefore controllers that use a PEPS and provider of PEPS services will have to decide if they consider themselves as a controller or processor under the Directive 95/46."*

[26] Zie Deliverable D2.2 Report on Legal Operability, p. 39. *"The most important ground to make the processing of personal data across state borders legitimate is unambiguous consent of the data subject (the claimant), because legal obligations (as meant in art. 7(c)) are unlikely to exist in a pan-European context. This requirement will not be much of a problem when the data is disclosed by the claimant herself (e.g., in an online form), or when data can be obtained from a certificate presented by the claimant (for instance, taken from a certificate on a smart card used by the claimant). It is more complicated when the service provider (relying party) needs to obtain additional data, such as (certified) attributes and these can be, or even have to be*

vooral te maken met issues rondom nationale persoonsnummers en het feit dat het om een onderzoekspilot ging. Voor het eIDAS-koppelpunt ligt dit geheel anders. Voor wat de grondslag betreft, lift de verwerking door het koppelpunt mee met de grondslag voor de e-overheidsdienstverlening waarvoor de authenticatie benodigd is. In de meeste gevallen zal de gegevensverwerking noodzakelijk zijn voor de goede uitvoering van een publiekrechtelijke taak door de dienstverlener in kwestie (artikel 7 sub e Richtlijn 95/46/EG en artikel 8 sub e Wbp) of er is sprake van een wettelijke plicht tot het aanleveren van de identiteitsgegevens bij de overheidsdienstverlener (artikel 7 sub c Richtlijn 95/46/EG en artikel 8 sub c Wbp). In beide gevallen hoeft de burger geen toestemming te geven voor de verwerking van zijn identiteitsgegevens aan de overheidsdienstverlener en dus ook niet door het koppelpunt. Dat geldt ook als het een overheidsdienstverlener betreft in een andere Lidstaat. Daar komt bij dat toestemming moet kunnen worden geweigerd of ingetrokken. Als weigeren of intrekken feitelijk geen optie is omdat er sprake is van een wettelijke plicht of het overheidsorgaan zijn publieke taak dan niet naar behoren zou kunnen uitvoeren, is het vragen van toestemming oneigenlijk en is er geen sprake van een geldige toestemming (art. 1 sub i Wbp). Toestemming zou ons insziens derhalve geen grondslag moeten zijn bij de verwerking van persoonsgegevens via het eIDAS-koppelpunt.[27]

> NB. Het is echter niet uitgesloten dat de betrokkene in de gelegenheid wordt gesteld om additionele identiteitsgegevens aan te leveren. In dat geval is diens ondubbelzinnige toestemming nodig voor de verwerking van die gegevens door het koppelpunt. Dit kan evenwel door het zelf invullen van de additionele identiteitsgegevens (actieve handeling), waarbij de betrokkene voldoende geïnformeerd wordt over het feit dat zijn gegevens – via het koppelpunt – zullen worden doorgegeven aan de bij de verwerking betrokken partijen (informatie). Een expliciete toestemmingshandeling, zoals het aanvinken van een toestemmingsvakje, kan dan derhalve achterwege blijven en hoeft dus ook niet technisch te worden ingericht. Wel moet in dat geval aan de gebruiker duidelijk worden gemaakt welke gegevens verplicht zijn en welke optioneel.[28]

- *Ad 4: Verenigbaar gebruik*
  Het eIDAS-koppelpunt geeft de gegevens slechts door. Er is geen sprake van ander gebruik van de persoonsgegevens door het koppelpunt en zulks gebruik is ook niet gepland.

- *Ad 5: Kwantiteit van de gegevens*
  Het eIDAS-koppelpunt verwerkt uitsluitend de identiteitsgegevens die door andere partijen worden aangeboden. Als zodanig is het koppelpunt dus niet verantwoordelijk

---

obtained, from other sources than the user. In some cases it may be possible to collect the data from authentic registers in the claimant's home state without the claimants' involvement. In these cases, the relying party still would have to ask the claimant's consent in order to make the processing legitimate."

[27] Voor de volledigheid wijzen wij er op dat dit een aspect deel zou moeten uitmaken van een adviesaanvraag over het wetsvoorstel aan het CBP teneinde over dit punt zekerheid te krijgen.

[28] Zie ook de Memorie van Toelichting op het wetsvoorstel 33 902 (aanpassing artikel 11.7a Telecommunicatiewet) voor de vraag wanneer er op internet sprake kan zijn van ondubbelzinnige toestemming.

voor de kwantiteit van de gegevens.

- *Ad 6: Bewaartermijn*
  Het eIDAS-koppelpunt slaat geen identiteitsgegevens op. Wel worden de loggegevens opgeslagen. Er moet nog een besluit genomen worden hoe lang die loggegevens worden bewaard. Artikel 9 lid 3 van de Implementatieverordening Interoperabiliteit zegt hierover: *The data shall be stored for a period of time in accordance with national requirements*. In Nederland bestaan voor zover wij weten geen voorschriften voor het bewaren van loggegevens, dus daarover zal – bij voorkeur door de wetgever – een besluit moeten worden genomen.

- *Ad 7: Kwaliteit van de gegevens*
  Het eIDAS-koppelpunt is niet verantwoordelijk voor de juistheid van de identiteitsgegevens die het doorgeeft. Dat zijn de partijen die de gegevens aanleveren.

- *Ad 8: Vertrouwelijke omgang met de gegevens*
  Omdat er nog geen implementatie is, kan ook geen uitspraak worden gedaan over de wijze waarop medewerkers van het koppelpunt omgaan met gegevens. De verwachting is overigens dat de medewerkers alleen versleutelde gegevens zien, maar dat moet in de praktijk nader worden vastgesteld (zie Aanbeveling 8 in Hoofdstuk 6).

- *Ad 9 en 10: Beveiligingsmaatregelen en datalekken*
  Het is onbekend welke beveiligingsmaatregelen precies worden getroffen, buiten hetgeen in de eIDAS-verordening en de uitvoeringshandelingen van de Europese Commissie hierover bepaald is. Dit komt enerzijds omdat de software wordt gebouwd door de Europese Commissie en anderzijds omdat nog onduidelijk is waar het eIDAS-koppelpunt precies wordt ondergebracht. Hetzelfde geldt voor het risico op datalekken.[29] (zie Aanbeveling 9 in Hoofdstuk 6)

- *Ad 11: Afspraken met de bewerker*
  Dit punt hangt samen met het antwoord op punt 1 en de vraag naar de hosting van het eIDAS-koppelpunt. Zolang niet duidelijk is wie de verantwoordelijke is voor het eIDAS-koppelpunt en ook waar het koppelpunt wordt ondergebracht, is onduidelijk óf er een bewerker is, en zo ja, welke afspraken er met die bewerker zijn gemaakt (zie Aanbeveling 7 in Hoofdstuk 6).

- *Ad 12: Bijzondere gegevens*
  De Wbp stelt grenzen aan de verwerking van bijzondere gegevens, zoals etniciteitsgegevens, medische gegevens en geloofsovertuiging (zie art. 16 Wbp).

---

[29] Voor de volledigheid nemen wij hier de opmerkingen op die de Artikel 29 Werkgroep heeft gemaakt met betrekking tot de informatiebeveiliging: *"However all communication is routed through the users browser and therefore the risk of a man-in-the-middel attack has to be taken into consideration for both models, especially in the PEPS model because of the post-redirection via the users browser. STORK should further make sure to counter the typical risks of the centralized architecture of the PEPS model where much more transactions are processed for each request. STORK should implement a continuous surveillance of the system to make sure to be able to discover and counter risks that occur during the transactions."*

Zolang het koppelpunt uitsluitend de verplichte minimale dataset en de definieerde optionele attributen verwerkt, worden er geen bijzondere gegevens verwerkt.

> N.B. Dit kan anders zijn als er in de toekomst aanvullende attributen worden doorgegeven (zie Aanbeveling 10 in Hoofdstuk 6).

- *Ad 13: BSN*
  Nederland zal geen burgerservicenummers (BSN's) verstrekken via het eIDAS-koppelpunt. In plaats daarvan wordt een van het BSN afgeleid uniek identiteitsnummer gebruikt bij het verstrekken van authenticatiegegevens naar andere lidstaten. Het is nog niet bekend waar de omzetting van het BSN gaat plaatsvinden, maar dit zal in ieder geval niet in het eIDAS-koppelpunt zelf zijn. Het koppelpunt verwerkt het BSN dus niet.

  Los van waar deze plaatsvindt, is een aandachtspunt de wettelijk basis voor de omzetting van het BSN. Op grond van artikel 24 lid 1 Wbp is daarvoor een expliciete wettelijke bepaling vereist.[30] Het wetsvoorstel bevat een dergelijke bepaling nu niet (zie Aanbeveling 2 in hoofdstuk 6).

- *Ad 14: Melding bij CBP of FG*
  In beginsel moet op grond van artikel 27 Wbp elke verwerking van persoonsgegevens worden gemeld bij het CBP of de Functionaris voor de Gegevensbescherming van de verantwoordelijke (als die er is). Als een bestuursorgaan ingevolge een wettelijke verplichting persoonsgegevens verwerkt, is de verplichting tot melding niet van toepassing (art. 29 lid 4 Wbp). Óf het koppelpunt moet worden gemeld, en zo ja bij wie, is afhankelijk van de vraag waar de verantwoordelijkheid voor het koppelpunt wordt belegd: bij de Minister va EZ of bij een of meer eID-makelaars. Dit zal nader moeten worden onderzocht.

- *Ad 15: Informatie aan betrokkene*
  Het is onbekend hoe de informatie aan de betrokkene over de verwerking van persoonsgegevens precies zal plaatsvinden. Logischerwijs gebeurt dit via het inlogscherm van de gevraagde dienst, maar dit staat nog niet vast. Daarnaast speelt een rol of en zo ja hoe de Europese implementatieoplossing van de Europese Commissie eisen zal stellen op dit punt.

> NB. De Artikel 29 Werkgroep heeft in haar brief inzake het STORK-project specifieke eisen gesteld aan de informatieplicht:
> "*We would further like to recommend the implementation of the following measures that we consider being important [...] to put in place a privacy friendly interoperability model system for transborder eID recognition in Europe:*
> *[...]*

[30] Aan het omzettingsproces en de systematiek van de afgeleide identiteitsnummers zijn bovendien nog een aantal eisen te stellen. Zie hiervoor paragraaf 2.2.3.2 van Stork1 Deliverable D5.7.3 Functional Design for PEPS, MW models and interoperability.

- *"Privacy notes that take into account the complex infrastructure should be made available. Due to the differences deriving from the choice of the middleware (MW) or the proxy (PEPS) model on both sides of the transaction, the notes should be made in a way that exactly explains what happens in every possible constellation and provide the end user with the appropriate version of the notes".* [31]

Deze nogal vergaande eisen van de gezamenlijke toezichthouders stellen het hele eIDAS systeem voor een flinke uitdaging. Nagedacht zal moeten worden hoe dit op een uniforme wijze in alle Lidstaten kan worden geïmplementeerd. Daar komt bij dat de informatie begrijpelijk moet zijn voor de betrokkene (zie ook de voorstellen voor de nieuwe Algemene Europese Verordening Gegevensbescherming op dit punt). Dat betekent in de praktijk dat de informatie in minimaal alle officiële talen van de Europese Unie beschikbaar moet zijn, ook in Nederland. Immers een belangrijk gebruiksscenario dat wij voorzien, is die van een burger van een andere Lidstaat die langere tijd in Nederland verblijft zonder in Nederland te zijn ingeschreven. Deze burger authentiseert zich in principe steeds met het eID van zijn thuisland bij Nederlandse overheidsdiensten. In dat geval zal het Nederlandse koppelpunt verbinding zoeken met het koppelpunt van de betreffende Lidstaat. De vereiste informatie zal hem in principe in zo'n geval in zijn eigen taal moeten worden aangeboden (hij zal althans de keus moeten hebben om van taal te wisselen), ook al meldt hij zich bij een Nederlandse overheidsdienst.

- *Nr. 16: Uitoefening rechten betrokkene*
  De betrokkene heeft het recht op inzage (art. 35 Wbp), correctie (art. 36 Wbp) en – in geval de verwerking plaatsvindt op basis van de publieke taak van een bestuursorgaan – het recht van verzet (art. 40 Wbp). Omdat de implementatie nog niet beschikbaar is, kunnen geen uitspraken gedaan worden de wijze waarop door de verantwoordelijke voor het koppelpunt invulling wordt gegeven aan deze rechten. Overigens verwachten wij dat gelet op de verwachte functionaliteit van het koppelpunt, de uitoefening van deze rechten in de praktijk weinig relevant zullen zijn.

- *Ad 17: Internationaal gegevensverkeer*
  Zolang het koppelpunt alleen communiceert met partijen binnen de Europese Economische Ruimte (EER), vindt er geen internationaal gegevensverkeer plaats als bedoeld in artikel 76 lid 1 Wbp.

[31] Zie Bijlage 3 bij dit rapport.

Hoofdstuk 6 – Aanbevelingen

In dit hoofdstuk doen wij een aantal aanbevelingen op het gebied van:

- wet- en regelgeving rondom het eIDAS-koppelpunt,
- de (toekomstige) inrichting van het eIDAS-koppelpunt, en
- het verdere verloop van het ontwikkeltraject.

I. Op het punt van **wet- en regelgeving** doen wij de volgende aanbevelingen:

Aanbeveling 1

Artikel 1 sub d Wbp schrijft voor dat er minimaal één verantwoordelijke is voor het eIDAS-koppelpunt.[32] De analyse van de Artikel 29 Werkgroep op het STORK-project laat zien dat er iets voor te zeggen valt dat de exploitant van een eIDAS-node een verantwoordelijke is vanwege zijn taken ('feitelijke verantwoordelijkheid'), maar ook dat deze een bewerker kan zijn voor de overheidsdienstverleners. Om aan deze discussie een eind te maken en helderheid te scheppen in wie nu eigenlijk de verantwoordelijke is en dus wie verantwoordelijk is voor de naleving van de verplichtingen van de Wbp, de rechten van de betrokkene moet waarborgen en aansprakelijk is als het mis gaat, adviseren wij om bij wet een verantwoordelijke voor het koppelpunt aan te wijzen. Dit is in lijn met het uitgangspunt dat verantwoordelijkheden daar moeten worden belegd waar dat de naleving van de regelgeving met betrekking tot gegevensbescherming in de praktijk voldoende is gewaarborgd.[33] Daarmee wordt deze partij een 'formele verantwoordelijke'.[34]

Er zijn dan drie basisvarianten mogelijk:

1) De Minister van EZ is de verantwoordelijke

De wet wijst in dit geval de Minister van EZ aan als verantwoordelijke in de zin van de Wbp. Er zijn dan een aantal subvarianten denkbaar:

a) *In-house oplossing:* De Minister van EZ is verantwoordelijke en de oplossing wordt binnen EZ gehost.
b) *Semi-inhouse oplossing:* De Minister van EZ is verantwoordelijke, maar de oplossing wordt elders binnen het Rijk gehost. Die overheidsinstantie wordt dan bewerker voor EZ.
c) *Externe oplossing:* De Minister van EZ is verantwoordelijke, maar de oplossing wordt bij een private partij gehost (bijv. een eID-makelaar). Die

---

[32] Artikel 2.5e van het wetsvoorstel bepaalt weliswaar dat de Minister van Economische Zaken verantwoordelijke is voor enkele verwerkingen die samenhangen met vertrouwensdiensten, maar dat is een ander onderwerp in de verordening, dat geen direct verband houdt met elektronische identificatie.

[33] Zie ook het Advies van de Artikel 29 Werkgroep inzake de begrippen 'verantwoordelijke' en 'bewerker' van 16 februari 2010 (WP 169).

[34] De artikel 29 Werkgroep spreekt in dat geval over een verantwoordelijke "op grond van een uitdrukkelijke juridische bevoegdheid", dat wil zeggen dat de voor de verwerking verantwoordelijke of de specifieke criteria voor zijn aanstelling zijn vastgelegd in nationale of communautaire wetgeving (Opinie van 16 februari 2010, WP169, pagina 12).

partij wordt dan bewerker voor EZ.

2) De eID-makelaar (of een andere private partij) is verantwoordelijke
De wet wijst in dit geval de private partij die voldoet aan specifieke criteria aan als verantwoordelijke in de zin van de Wbp. De Minister van EZ is alleen nog beleidsverantwoordelijk, maar geen ‘verantwoordelijke’ in de zin van de Wbp.

3) De overheidsdienstverleners die gebruik maken van eID zijn de verantwoordelijke
In deze variant is de exploitant van het eIDAS-koppelpunt slechts een bewerker voor de aangesloten partijen. Deze variant werd door de Artikel 29 Werkgroep als mogelijkheid geopperd.[35] Een bewerkersrol voor het koppelpunt past ons insziens echter niet vanwege het feit dat de Wbp voorschrijft dat de verantwoordelijke toezicht moet houden op de bewerker (art. 14 lid 1) en dat de verantwoordelijke instructies mag/moet geven aan de bewerker (art. 14 lid 3 juncto artikel 12 lid 1). Dat impliceert dat er een relatie is tussen de verantwoordelijke en de bewerker waarin deze rechten van de verantwoordelijke ook geoperationaliseerd kunnen worden. Van dat laatste zal geen sprake zijn als het koppelpunt bewerker is voor de partijen die daarop zijn aangesloten. Daarnaast brengt deze variant aanzienlijke administratieve lasten met zich mee, omdat er met heel veel partijen afspraken moeten worden gemaakt. Bovendien is het waarschijnlijk niet goed mogelijk om bij Nederlandse wet een buitenlandse overheidsdienstverlener te benoemen tot verantwoordelijke. Daarom raden wij deze variant af.

Welke variant gekozen wordt, is vooral afhankelijk van de vraag wie (in juridische zin) de regie over het koppelpunt zal moeten gaan voeren en dus de kaders mag stellen (anders dan bij wet- en regelgeving) waarbinnen de gegevens worden verwerkt. Deze partij is dan verantwoordelijk voor de nakoming van de verplichtingen van de Wbp en het waarborgen van de rechten van de betrokkenen. Daarnaast is hij aansprakelijk voor de schade of het nadeel dat voortvloeit uit het niet-naleven van die verplichtingen, zelfs als die schade of dat nadeel is veroorzaakt door de bewerker.

Aanbeveling 2

Het omzetten van het BSN in een andere unieke identifier is een verwerking die een grondslag moet hebben in de wet (art. 24 Wbp). Derhalve bevelen wij aan om de omzetting van het BSN ten behoeve van de verwerking via het eIDAS-koppelpunt een expliciete wettelijke basis te geven.

Aanbeveling 3

De informatie aan de betrokkene over de privacyaspecten van de eIDAS-koppelpunten zou in Europa in principe overal hetzelfde moeten zijn. Daarnaast zou – gelet op het

[35] Dit was ook de variant die wordt gebruikt door SWIFT dat het berichtenverkeer in het internationale bankwezen afhandelt. In dat geval hebben we echter gezien dat die rol al snel kan omslaan tot verantwoordelijke. Zie Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

grensoverschrijdende karakter van de verwerking – de informatie in alle officiële talen van de Unie beschikbaar moeten zijn. Ook zal de informatie via de aangesloten overheidsdienstverleners moeten worden verstrekt omdat het koppelpunt geen interface heeft om met de betrokkene te communiceren. Wij bevelen daarom aan om de te verstrekken informatie over de privacyaspecten van het koppelpunt op Europees niveau in regelgeving vast te leggen.

Aanbeveling 4

Momenteel stellen de Lidstaten zeer uiteenlopende eisen aan de beveiliging van verwerkingen van persoonsgegevens. Daardoor dreigt een lappendeken te ontstaan van beveiligingsmaatregelen, waardoor de identiteitsgegevens in de ene Lidstaat anders worden beveiligd dan in de andere Lidstaat. Dat is gelet op het Europese karakter van het netwerk niet logisch. Wij bevelen daarom aan om de beveiligingseisen voor de koppelpunten gedetailleerd uit te werken op Europees niveau en deze bindend op te leggen aan de Lidstaten.

Aanbeveling 5 *(voor zover Aanbeveling 4 niet wordt gevolgd)*

Indien het eIDAS-koppelpunt wordt ondergebracht bij een of meer eID-makelaars, bevelen wij – gelet op het feit dat beveiliging van het gegevensverkeer door het koppelpunt de belangrijkste zorg is als het gaat om de privacyrisico's van de betrokkene – aan om specifieke minimumeisen te stellen op het gebied van informatiebeveiliging die door deze makelaars moeten worden geïmplementeerd. Het kan gaan om technische eisen, maar ook om organisatorische eisen (bijv. periodieke audits).

Als de Minister de verantwoordelijke is en de eID-makelaar de bewerker voor het eIDAS-koppelpunt dan dienen deze eisen in de aanbesteding en de bewerkersovereenkomst worden neergelegd. Bij de aanbesteding dienen de beveiligingseisen een knock-out criterium te zijn.

Aanbeveling 6

Artikel 7 sub f eIDAS-verordening laat toe dat Lidstaten voorwaarden stellen aan andere vertrouwende partijen dan openbare diensten. Wij adviseren de eisen rondom privacy en security, waaronder het uitvoeren van een privacy impact assessment en/of risicoanalyse op het gebied van informatiebeveiliging, onderdeel uit te laten maken van de aansluitvoorwaarden op het eIDAS-koppelpunt.

II. Op het punt van de toekomstige **inrichting van het eIDAS-koppelpunt** doen wij de volgende aanbevelingen:

Aanbeveling 7

Alvorens het eIDAS-koppelpunt wordt ondergebracht bij een of meer private partijen, bevelen wij aan om een risico-evaluatie uit te voeren op de door die partijen geboden technische en bestuurlijke omgeving.

Dit geldt ook voor het geval de eIDAS-node bij EZ zelf wordt ondergebracht. In dat laatste geval bevelen wij aan om een Wbp-coördinator van EZ en de Functionaris voor de Gegevensbescherming van EZ betrokken te betrekken bij de implementatie.

Aanbeveling 8

De keuze tussen end-to-end encryptie en encryptie per schakel in de keten is nog open. End-to-end encryptie heeft het voordeel dat de gegevens niet toegankelijk zijn voor het koppelpunt, waardoor het risico van datadiefstal of misbruik van data de medewerkers vormen wordt verkleind.

In ieder geval, maar zeker als er sprake is van encryptie per schakel, dienen passende maatregelen te worden genomen om deze risico's te verminderen. Deze maatregelen dienen in ieder geval te betreffen:

- Het opleggen van een geheimhoudingsplicht;
- Het vragen van een Verklaring omtrent het gedrag (VOG);
- Het toepassen van functiescheiding en *least privilege*;
- Het loggen van de toegang tot het systeem en de verrichte handelingen; en
- Bewustwording op het gebied van informatiebeveiliging.

Een grondige risicoanalyse op het gebied van informatiebeveiliging alvorens het systeem live gaat zal mogelijk nog tot aanvullende maatregelen op het gebied van *human resource security* leiden.

III. Op het punt van het verdere verloop van het **ontwikkeltraject van het eIDAS-koppelpunt** doen wij de volgende aanbevelingen:

Aanbeveling 9

Een belangrijk deel van de privacy- en securityaspecten van het eIDAS-koppelpunt wordt ingevuld door de referentie-implementatie en de software die door de Europese Commissie wordt ontwikkeld. Voor zover dit nog niet gedaan is, bevelen wij aan dat op Europees niveau alsnog een PIA, inclusief risico-evaluatie op het gebied van de informatiebeveiliging, op die referentie-implementatie en de software wordt uitgevoerd.

Aanbeveling 10

Omdat met het toelaten van aanvullende attributen de privacyrisico's van het eIDAS-koppelpunt mogelijk kunnen wijzigen, met eventuele gevolgen voor de te implementeren maatregelen, adviseren wij om telkens bij de toelating van dergelijke attributen een aanvullende PIA uit te voeren.

Bijlage 1 – Vragenlijst Toetsmodel PIA Rijksdienst

NB. *Deze vragenlijst is gebruikt bij de intake van het PIA-project en vormt de basis voor de beschrijving van de verwerking van het eIDAS-koppelpunt in hoofdstuk 4 van deze PIA. Omdat het gebruik van deze vragenlijst voor de Rijksoverheid verplicht is, voegen wij de antwoorden van EZ voor de volledigheid toe als bijlage. Wij wijzen er op dat wij deze vragenlijst niet hebben bijgewerkt na de 2e workshop. Voor zover er verschillen mochten zijn tussen de beschrijvingen in de PIA en deze vragenlijst, geldt de beschrijving in de PIA.*

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type? (Zie paragraaf 4.2)

Het is een discussiepunt of de functionele beheerder van het eIDAS-koppelpunt een verantwoordelijke of bewerker is.
De Artikel 29 Werkgroep heeft aangegeven dat hier twee mogelijkheden zijn:
1) het eIDAS-koppelpunt is bewerker voor alle dienstverleners die er gebruik van maken
2) het eIDAS-koppelpunt is medeverantwoordelijke voor de gegevensverwerking.
In de PIA zullen we de voor- en nadelen van beide opties schetsen en trachten om op dit punt positie te bepalen. In beide gevallen is ook relevant welke organisatie (als bewerker c.q. medeverantwoordelijke) het koppelpunt gaat beheren.

Bijzonder aandachtspunt is de software die vanuit MW-landen (Duitsland, Oostenrijk) op het eIDAS-koppelpunt geplaatst wordt.[36] Zie ook het aandachtspunt genoemd onder vraag 15.

De typen persoonsgegevens die gebruikt kunnen worden voor de verwerking, zijn uiteengezet in de eIDAS verordening. De minimale dataset bestaat uit:

- achternaam;
- voornaam/-namen;
- geboortedatum en
- unieke identifier.

Als optionele attributen die verwerkt mogen worden noemt de eIDAS verordening het volgende:

- voor- en achternamen bij geboorte;
- geboorteplaats;
- huidig (woon)adres en
- geslacht.

Daarnaast kunnen Lidstaten met elkaar afspraken maken om allerlei additionele attributen toe te voegen.

[36] N.B. Dit is ook van belang bij de beantwoording van enkele van de overige vragen.

2. **Andere specifieke persoonsgegevens?**
   a. **Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?**
   Nee. Het is in beginsel mogelijk (hoewel zeker op afzienbare termijn niet heel waarschijnlijk) dat zulke gegevens door attribuutdienstverleners via het koppelpunt doorgegeven worden. Het koppelpunt geeft deze gegevens overigens louter door aan de dienstverlener.

   b. **Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?**
   Neen. Zie onder (a).

   c. **Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?**
   Het is niet de bedoeling dat inloggegevens (gebruikersnamen, wachtwoorden) verwerkt worden door het eIDAS-koppelpunt. Dergelijke gegevens worden primair verwerkt door de identiteitsdienstverlener.

   d. **Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?**
   Nee. Dergelijke gegevens worden alleen verwerkt door de identiteitsdienstverlener.

   e. **Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken? (Zie 4.2.c)**
   Het is alleen de bedoeling om pseudoniemen (versleuteld) van het BSN te verwerken (pseudo-ID). De verwerking (het pseudonimiseren) van het BSN is alleen toegestaan voor doeleinden die expliciet in de Nederlandse wet vermeld staan. Zowel gepseudonimiseerde BSN's (bij grensoverschrijdende dienstverlening aan Nederlandse ingezetenen) als buitenlandse persoonsgebonden nummers (bij grensoverschrijdende dienstverlening door Nederlandse dienstverleners) kunnen verwerkt worden. Het pseudonimiseren zal plaats moeten vinden voordat de gegevens via de centrale eIDAS-node naar de (buitenlandse) dienstverlener verstuurd wordt.

   NB. Pseudoniemen worden in het algemeen nog steeds geacht persoonsgegevens te zijn, omdat ze een individu in een groep uniek kunnen aanwijzen (linkability). Pseudonimiseren in slechts een beveiligingsmaatregel.

3. **Kan van elk van de onder vraag 1 en vraag 2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken**

persoonsgegeven toe.
Deze vragen zijn voor het overgrote deel niet relevant, aangezien de gegevensverwerking door het koppelpunt goeddeels een vast gegeven is op basis van de eIDAS-verordening en de specificaties van de diensten van identiteitsdienstverleners. Dit ligt anders voor persoonsgebonden nummers. Daarvoor is het technisch mogelijk om ze te vertalen naar een contextafhankelijk pseudoniem. Tevens is de minimale dataset vastgelegd in de eIDAS verordening, terwijl de aanvullende attributen nog in de toekomst aangekondigd/gewijzigd kunnen worden. De toekomstige aanvullende attributen zijn dan ook out-of-scope voor deze PIA.

4. **Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?**
Zie antwoorden op de vorige twee vragen. Diverse persoonsgegevens zullen niet tot de minimale dataset behoren maar aangemerkt worden als een vrijwillige attribuut omdat landen verschillende visies hanteren omtrent de gevoeligheid van het desbetreffende type persoonsgegeven (bijvoorbeeld stigmatisering op basis van je geboorteplaats). Het platform moet zodanig robuust worden vormgeven dat het flexibel om kan gaan met diverse soorten persoonlijke gegevens (vrijwillige attributen) en tegelijkertijd ook aan de daaraan gestelde veiligheidseisen voldoet.

5. **In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?**

Hier gaan de eIDAS verordening en het concept wetsvoorstel wijziging Telecommunicatiewet over. Het idee is om het door de Europese Commissie ontwikkelde software te implementeren in Nederland. Zowel de verordening als de software zijn, voor zover het de standaardmodules betreft, out-of-scope voor deze PIA.

6. **Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel? (Zie paragraaf 4.3)**
Doel van het koppelpunt is het faciliteren van grensoverschrijdende dienstverlening binnen de EU/EER door het routeren van het daarvoor benodigde gegevensverkeer over authenticatie (authenticatiedienst) van burgers en bedrijven richting overheidsdienstverleners en mogelijk in de toekomst ook naar private partijen om bij deze partijen in het buitenland in te loggen met hun nationale eID middel (eHerkenning, DigiD, eIDstelsel (toekomst), zodat NL kan voldoen aan de EU verordening elektronische identiteiten en vertrouwensdiensten, eIDAS.

7. **Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).**
8. **Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?**
   Antwoord op de vragen 7 en 8: Het is een beetje van allebei. Vanuit de optiek van de identiteitsdienstverlener gaat het om het gebruik van bestaande persoonsgegevens voor nieuwe doeleinden, te weten (het mogelijk maken van) grensoverschrijdende dienstverlening. Vanuit de optiek van de dienstverlener gaat het om het gebruik van nieuwe persoonsgegevens (namelijk die van burgers uit andere lidstaten) voor bestaande doeleinden (mogelijk maken van het langs elektronische weg verlenen van diensten).

9. **Indien u positief hebt geantwoord op vragen 7 of 8, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?**
   Dit hangt af van het antwoord op vraag 1. Indien ervoor wordt gekozen dat het koppelpunt een bewerkersrol krijgt, dan hoeft het niet als zelfstandige verwerking gemeld te worden (de functie van de bewerker zal hoofdzakelijk informatiebeveiliging zijn). Indien ervoor wordt gekozen dat het koppelpunt medeverantwoordelijke is, dan zal zijn verwerking gemeld moeten worden bij het CBP of, indien van toepassing en gewenst, bij de FG van de verantwoordelijke. Vooralsnog moet eerst bepaald worden of de Minister van EZ verantwoordelijke zal zijn.

10. **Indien u positief geantwoord hebt op vragen 7 of 8, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?**
    Dit is nader te inventariseren. De controles zullen deels gedicteerd worden door de eIDAS-verordening en eventuele Implementing Acts.

11. **Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?**
    Aangezien het koppelpunt slechts een doorgifterol vervult, gaat het hier alleen om informatiebeveiliging. Zie daarvoor de vragen 21 en verder. Verder wordt alles via de Europese regelgeving geregeld. Omdat het definitieve koppelpunt nog moet worden gebouwd, kunnen er nu geen uitspraken gedaan worden over de wijze waarop en mate

waarin het koppelpunt voldoet aan de Europese normen die relevant zijn voor privacy en informatiebeveiliging.

12. **Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld? (Zie paragraaf 4.2.d)**
    Nee.

13. **Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?**
    N.v.t.

14. **Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder 5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?**
    Zie plaatje in Bijlage 3.

15. **Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht? (Zie paragraaf 4.1 en Aanbeveling 1)**
    Zie het antwoord op vraag 1: is de functionele beheerder een verantwoordelijke of een bewerker? Als de functionele beheerder de verantwoordelijke is, dan is het antwoord op deze vraag duidelijk: de functionele beheerder. Maar als deze een bewerker is, is op voorhand niet duidelijk wie dan wél de verantwoordelijke is. Daarnaast is niet nog niet duidelijk of het koppelpunt wordt ondergebracht bij EZ of bij een of meer eID-makelaars. Daarom kan nu nog niet specifiek een verantwoordelijke worden aangewezen.

    Vraag is overigens in hoeverre het nodig is dat het koppelpunt invloed uitoefent op c.q. eisen stelt (en welke dan) aan andere betrokken partijen in de keten.

    Met betrekking tot Duitsland en Oostenrijk (de zgn 'middleware landen'): het is de bedoeling dat deze landen een plug-in (middleware) gaan plaatsen op de Nederlandse

server waar de NL EU node staat. De functionele beheerder is dan bewerker voor de Duitse en Oostenrijkse verantwoordelijken.[37]

Als het koppelpunt bij EZ wordt ondergebracht, is de Baseline Informatiebeveiliging Rijksdienst (BIR) op het koppelpunt van toepassing. De BIR bevat een groot aantal beheersmaatregelen die moeten/kunnen worden genomen om het koppelpunt te beheren.

16. **Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden? (Zie paragraaf 4.8)**
    Afhankelijk van hoe lang de encryptieketen is, zal mogelijk niemand (koppelpunt moet gezien worden als doorgifteluik/regisseur van versleutelde gegevens), maar mogelijk alleen de technisch beheerder van het eIDAS-koppelpunt de (versleutelde) persoonsgegevens in kunnen zien. De technisch beheerder heeft dan een monitoring rol en zal een audit trail uit moeten kunnen voeren om het koppelpunt technisch fit te houden (zie ook art. 9 lid 3 van de concept-Uitvoeringshandeling Interoperabiliteit).

17. **Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?**
    Nee. In de toekomst kan dit per type dienstverlener verschillen, maar dat is nu out of scope.

18. **Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?**
    (Zie plaatje in Bijlage 3) Hierbij moet rekening gehouden worden met de vraag of de versleutelde data via de browser geredirect wordt van provider naar dienstverlener (na user consent) zonder dat de eIDAS node ‘fysiek’ de data door hoeft te sturen. De transmissie wordt wel geregistreerd (logging) door de eIDAS node. Technisch gezien is de node dan geen doorgeefluik. De node stuurt dan identificaties door naar de browser, zodra hij hoort naar welke dienstverlener het verzoek moet. Het is vooralsnog onduidelijk of de data ook ‘fysiek’ langs de eIDAS node zal gaan (waarschijnlijk niet, maar zolang de Europese software niet klaar is, kan dat niet worden uitgezocht).

    NB. Indien er om toestemming wordt gevraagd aan de gebruiker voor transmissie van zijn gegevens aan (buitenlandse) dienstverleners zal duidelijk moeten worden (in begrijpbare taal/B1 niveau) waar toestemming voor gegeven wordt en wat consequenties

[37] Het voert in het kader van deze PIA te ver om onderzoek te doen naar de eisen die de Duitse en Oostenrijkse wet stellen aan bewerkers. In het algemeen kan worden gesteld dat zowel Duitsland als Oostenrijk vergelijkbare eisen stellen aan bewerkers als de Nederlandse Wbp en de Richtsnoeren Beveiliging Persoonsgegevens van het CBP tezamen. Bovendien zullen die eisen vooral afhangen van de SLA’s die gesloten zullen (moeten) worden tussen Nederland en Duitsland resp. Nederland en Oostenrijk. Het ligt in de lijn der verwachting dat de eisen in die SLA’s de algemene wettelijke eisen nader zullen specificeren.

kunnen zijn indien er geen toestemming wordt afgegeven. Laatstgenoemde wordt ook voorgeschreven door de nieuwe Europese privacy verordening, waar DIGIT bij betrokken is (DG Informatics van de Europese Commissie die de software maakt, beheert en oplevert).

19. **Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?**
Nog niet. In beginsel ook niet van toepassing, aangezien het om doorgifte gaat. Uitzondering vormen in ieder geval wel de logbestanden, deze worden door Brussel voorgeschreven. In het geval van een onderaannemer moeten er afspraken in bewerkersovereenkomsten opgenomen worden.

20. **Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven? (Zie paragraaf 4.12)**
Nee, de rol van het koppelpunt is beperkt tot uitwisseling van authenticatiegegevens tussen partijen in lidstaten van de EU/EER.
Er vindt wel een uitwisseling plaats met Turkije, maar deze valt buiten de scope van de onderhavige PIA.

21. **Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging ? (Zie paragraaf 4.9)**
Dit moet blijken uit de uitvoeringshandeling. De Baseline Informatiebeveiliging Rijksdienst (BIR) is van toepassing voor governance. Zowel als bij zelf doen als bij uitbesteden. Maar het is op dit moment nog niet bekend waar dit nog allemaal moet plaatsvinden. Eventuele maatregelen moeten vooralsnog vanuit Europa bekend worden gemaakt (tenzij lidstaten dit zelf mogen bepalen).

22. **Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker? (Zie paragraaf 4.10)**
Nog niet bekend of het koppelpunt een (sub)bewerker gaat inschakelen. Aandachtspunt voor inrichten koppelpunt en toedelen van verantwoordelijkheid daarvoor. Indien het koppelpunt zelf als bewerker gaat optreden, dan is na te gaan hoe het toezicht daarop effectief geregeld kan worden, zeker aangezien er sprake zal zijn van vele verantwoordelijken, verspreid over de EU (ervan uitgaande dat het koppelpunt ook eID-

identiteiten zal gaan ontsluiten voor het verlenen van diensten vanuit andere lidstaten).

23. **Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen? (Zie paragraaf 4.9)**
De BIR is van toepassing op de Nederlandse implementatie, maar er zijn een aantal eisen aan de versleuteling en die komen uit Brussel.

24. **Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen? (Zie paragraaf 4.9)**
    - *uitzoeken.*
      eIDAS verordening gaat hierover (en de wettekst van de Telecommunicatiewet). Is nader te bepalen. Aandachtspunt voor inrichten koppelpunt. In de PIA is na te gaan of het soort verwerking en de context waarin die plaatsvindt specifieke eisen stelt op dit punt. De meldplicht datalekken in het Wbp wordt als tekst gewijzigd. Als er niets geregeld is dan moet dat nog gebeuren, in samenspraak met de desbetreffende partijen die het gaan uitbouwen op basis van de BIR voorschriften.
    - **Datalekken & de BIR**: het enige relevante gevonden artikel in de BIR m.b.t. datalekken is mogelijk artikel 12.5.4 omtrent '*het lekken van informatie: 'Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken. 1. Op een grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats.'*

25. **Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring? (Zie ad. 6 in Hoofdstuk 5 – Conclusie)**
Er wordt waarschijnlijk niets opgeslagen op de loggegevens na (gegevens zullen niet geregistreerd worden). Maar dit is pas nader te bepalen als de software klaar is. De eIDAS-verordening bevat hier bepalingen over. Mogelijk wordt er data in de technische cache opgeslagen als back-up?

26. **Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?**
Bewaring is noodzakelijk om betwiste transacties te kunnen reconstrueren en zo rechtszekerheid te kunnen bieden. De noodzakelijke lengte van de bewaartermijn is nader te bepalen, en zal waarschijnlijk mede volgen uit lagere regelgeving onder de eIDAS-

verordening (die er zelf niets over zegt)/Implementing Act. Op de audit-rail zal iets aangetoond moeten kunnen worden.

27. **Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief loggegevens, vernietigd? Is er controle op de vernietiging, en door wie?**
Nog niet bekend. Aandachtspunt voor inrichten koppelpunt. In de PIA is na te gaan of het soort verwerking en de context waarin die plaatsvindt specifieke eisen stelt op dit punt. Zal met de BIR in de hand en de Wbp coördinator van EZ moeten worden nagegaan.

28. **Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens? (Zie paragraaf 4.11)**
Het doel van de gegevensverwerking mag in beginsel bekend verondersteld worden, te weten het mogelijk maken van het verlenen van de door de betrokkene verzochte dienst. Nadere informatie over de authenticatieprocedure en de rol van het koppelpunt daarin kan wel wenselijk zijn. Vgl. ook het antwoord op vraag 18. Er zijn twee manieren voor de betrokkene om te weten wat er gebeurt. Via het scherm waarmee toestemming gegeven wordt (de platform bouwers zullen hiermee rekening moeten houden). En de overheidsdienstverleners hebben ook een informatieplicht (nationale wetgeving).

29. **Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?**
N.v.t.

30. **Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?**
Zie vraag 28. Dit is nader uit te werken. Dit kan deels bij de dienstaanbieder, deels bij het koppelpunt gelegd worden..

31. **Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?**
Intrekken van toestemming is niet van toepassing omdat toestemming eenmalig verstrekt is/door aard van de informatieverwerking. Met betrekking of de betrokkene begrijpt wat de implicaties zijn, is voor aandacht van de Europese Commissie (hoort bij het scherm). In de eerste plaats is het de vraag in hoeverre überhaupt gewerkt wordt met toestemming als grondslag: noodzaak voor uitvoering van een overeenkomst lijkt waarschijnlijker. Mogelijk kan er een instructie aan overheidsdienstverleners afgegeven worden dat zij een voor de 'gebruiker' duidelijke en toegankelijk traject beschikbaar hebben voor het

indienden van een verzoek tot intrekken van de afgegeven toestemming?

32. **Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?**
Inzage in de minimale basisset is niet aan de orde omdat het gaat om een eenmalige verstrekking. De basisset volgt uit de verordening, welke voor eenieder toegankelijk is. Inzage, correctie en verzet vindt feitelijk plaats bij de dienstverlener en niet bij het koppelpunt.

33. **Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?**
Zie het antwoord op de vorige vraag. Vraag 32.

Bijlage 2

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) is van toepassing op de ‘geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens’. Uit de Wbp vloeien in hoofdlijnen de volgende rechten en verplichtingen voort:

- De persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt;

- Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld;

- Persoonsgegevens mogen slechts worden verwerkt indien de verantwoordelijke daartoe een grondslag heeft (bijv. toestemming van de betrokkene, een wettelijke plicht, uitvoering van een publiekrechtelijke taak, of het gerechtvaardigd belang van de verantwoordelijke dat het (privacy)belang van de betrokkene overstijgt);

- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden, wordt niet als onverenigbaar beschouwd, indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden;

- Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Persoonsgegevens mogen langer worden bewaard voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt;

- Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn;

- De verantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn;

- Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke;

- De personen die toegang hebben tot persoonsgegevens en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen;

- De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen;

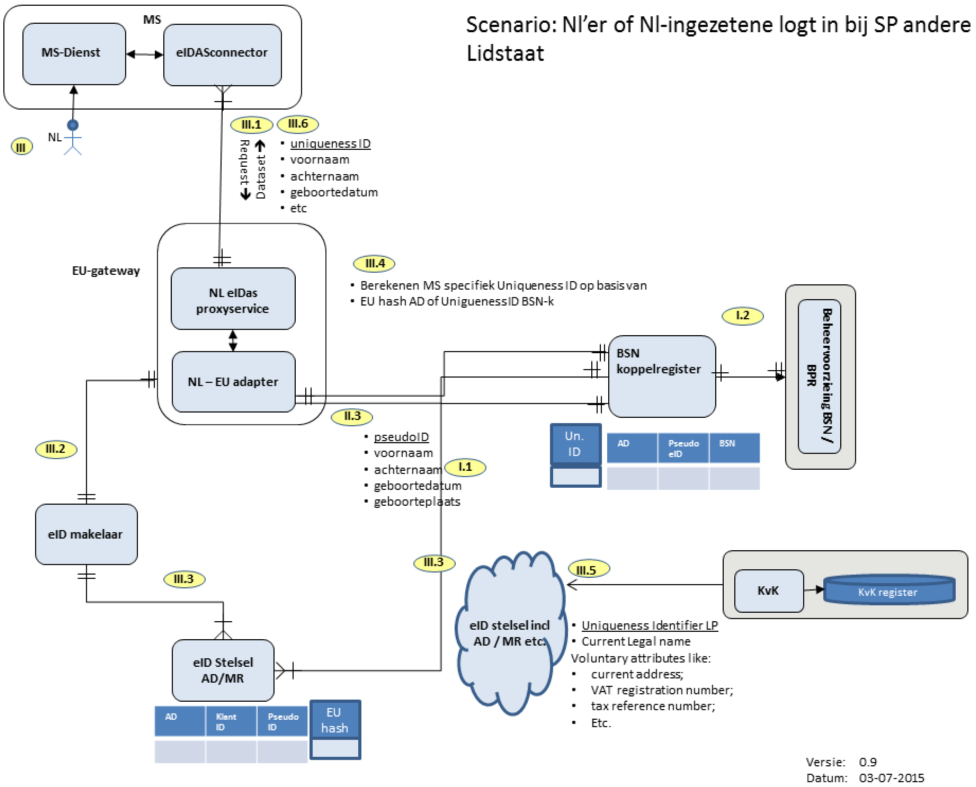
- Indien de verantwoordelijke persoonsgegevens laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen. De uitvoering van verwerkingen door een bewerker wordt geregeld in een schriftelijke overeenkomst of krachtens een andere schriftelijk vastgelegde rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke;

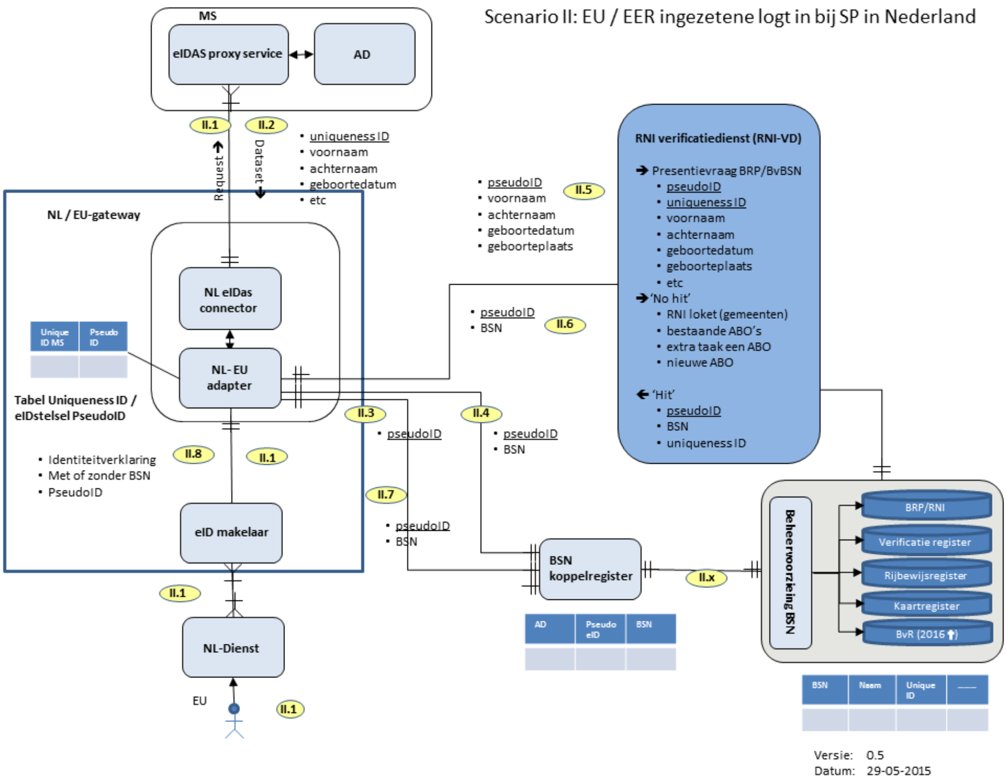
- De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in artikelen 17 t/m 23 Wbp. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de medewerker zijn identiteit en de doeleinden van de verwerking mee alsmede nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

- De betrokkene heeft met betrekking tot de door de verantwoordelijke verwerkte persoonsgegevens een recht op inzage, correctie, afscherming en verzet.

Bijlage 3 – Schematisch overzicht datastromen





Bijlage 4 – Brief Artikel 29 Werkgroep inzake het STORK-project

/

Ref. Ares(2011)424406 - 15/04/2011

ARTICLE 29 Data Protection Working Party

Brussels, 15 April 2011
just.c3(2011) 471117

ATOS Origin
Antonio Paradell
Av. Diagonal 200
08018 Barcelona
Spain

Dear Mr. Paradell,

On behalf of the Article 29 Working Party I would like to thank you for the cooperation and assistance the STORK project partners gave to the Working Party when it came to understand the technical and organisational details of the STORK project.

We would like to share with you our conclusions and therefore attach to this letter the written report dealing with the STORK project from a data protection point of view. We would further like to recommend the implementation of the following measures that we consider being important in the context of your efforts to put in place a privacy friendly interoperability model system for transborder eID recognition in Europe:

- Although the confidentiality of the log files is protected by several encryption layers the retention period should be defined according to the time technically necessary to repair the system or other similar activities.

- A comparative privacy risk analysis between the PEPS and the MW model should be carried out. Apparently one model requires architecture with a significantly higher number of data transfers and it seems that a lot of effort is required to make those 2 models interoperable. That's why we suggest carrying out a comparative risk analysis that should clarify which are the specific risks of both models and why from a technical point of view both models need to be implemented although they apparently deliver the same result.

- Guidelines that give specific recommendations on common minimum standards on data security and on how the principle of proportionality and data minimisation should be transposed in the field of requesting additional attributes through STORK should be developed.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

- Privacy notes that take into account the complex infrastructure should be made available. Due to the differences deriving from the choice of either the MW or PEPS model on both sides of the transaction, the notes should be made in a way that exactly explains what happens in every possible constellation and provide the end user with the appropriate version of the notes.

- Security certificates used should be from a locally known and trusted provider.

Last but not least, the Article 29 Working Party would be grateful to be involved in a possible follow-up project in an earlier stage of the project.

Yours sincerely,

Jacob Kohnstamm
Chairman

Enclosure: Written report of the Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup